PRIVACY IMPACT ASSESSMENT (PIA)

For the

Defense Civilian Personnel Data System (DCPDS)

DHRA/Civilian Personnel Management Service (CPMS)

SECTION 1: IS A PIA REQUIRED?

a. Will this Department of Defense (DoD) information system or electronic collection of information (referred to as an "electronic collection" for the purpose of this form) collect, maintain, use, and/or disseminate PII about members of the public, Federal personnel, contractors or foreign nationals employed at U.S. military facilities internationally? Choose one option from the choices below. (Choose (3) for foreign nationals).

☐ (1) Yes, from members of the general public.

☒ (2) Yes, from Federal personnel* and/or Federal contractors.

☐ (3) Yes, from both members of the general public and Federal personnel and/or Federal contractors.

☐ (4) No

* "Federal personnel" are referred to in the DoD IT Portfolio Repository (DITPR) as "Federal employees."

b. If "No," ensure that DITPR or the authoritative database that updates DITPR is annotated for the reason(s) why a PIA is not required. If the DoD information system or electronic collection is not in DITPR, ensure that the reason(s) are recorded in appropriate documentation.

c. If "Yes," then a PIA is required. Proceed to Section 2.

SECTION 2: PIA SUMMARY INFORMATION

a. Why is this PIA being created or updated? Choose one:

- ☐ **New DoD Information System**
- ☐ **New Electronic Collection**
- ☒ **Existing DoD Information System**
- ☐ **Existing Electronic Collection**
- ☐ **Significantly Modified DoD Information System**

b. Is this DoD information system registered in the DITPR or the DoD Secret Internet Protocol Router Network (SIPRNET) IT Registry?

- ☒ **Yes, DITPR** Enter DITPR System Identification Number: 91
- ☐ **Yes, SIPRNET** Enter SIPRNET Identification Number:
- ☐ **No**

c. Does this DoD information system have an IT investment Unique Project Identifier (UPI), required by section 53 of Office of Management and Budget (OMB) Circular A-11?

- ☒ **Yes**
- ☐ **No**

If "Yes," enter UPI 007-97-01-11-01-0573-00-403-252

If unsure, consult the Component IT Budget Point of Contact to obtain the UPI.

d. Does this DoD information system or electronic collection require a Privacy Act System of Records Notice (SORN)?

A Privacy Act SORN is required if the information system or electronic collection contains information about U.S. citizens or lawful permanent U.S. residents that is retrieved by name or other unique identifier. PIA and Privacy Act SORN information should be consistent.

- ☒ **Yes**
- ☐ **No**

If "Yes," enter Privacy Act SORN Identifier DPR 34

DoD Component-assigned designator, not the Federal Register number.
Consult the Component Privacy Office for additional information or
access DoD Privacy Act SORNs at: http://www.defenselink.mil/privacy/notices/

or

Date of submission for approval to Defense Privacy Office
Consult the Component Privacy Office for this date.

e. Does this DoD information system or electronic collection have an OMB Control Number?
Contact the Component Information Management Control Officer or DoD Clearance Officer for this information.

This number indicates OMB approval to collect data from 10 or more members of the public in a 12-month period regardless of form or format.

☐ **Yes**

Enter OMB Control Number

Enter Expiration Date

☒ **No**

f. Authority to collect information. A Federal law, Executive Order of the President (EO), or DoD requirement must authorize the collection and maintenance of a system of records.

(1) If this system has a Privacy Act SORN, the authorities in this PIA and the existing Privacy Act SORN should be the same.

(2) Cite the authority for this DoD information system or electronic collection to collect, use, maintain and/or disseminate PII. (If multiple authorities are cited, provide all that apply.)

(a) Whenever possible, cite the specific provisions of the statute and/or EO that authorizes the operation of the system and the collection of PII.

(b) If a specific statute or EO does not exist, determine if an indirect statutory authority can be cited. An indirect authority may be cited if the authority requires the operation or administration of a program, the execution of which will require the collection and maintenance of a system of records.

(c) DoD Components can use their general statutory grants of authority ("internal housekeeping") as the primary authority. The requirement, directive, or instruction implementing the statute within the DoD Component should be identified.

5 U.S.C. 301, Department Regulations; 5 U.S.C. Chapters 11, 13, 29, 31, 33, 41, 43, 51, 53, 55, 61, 63, 72, 75, 83, 99; 5 U.S.C. 7201, Antidiscrimination Policy; 10 U.S.C. 136, Under Secretary of Defense for Personnel and Readiness; Executive Order 9830, Amending the Civil Service Rules and Providing for Federal Personnel Administration, as amended; Executive Order 9397 (SSN); and 29 CFR 1614.601, EEO Group Statistics.

g. Summary of DoD information system or electronic collection. Answers to these questions should be consistent with security guidelines for release of information to the public.

(1) Describe the purpose of this DoD information system or electronic collection and briefly describe the types of personal information about individuals collected in the system.

To establish a system of records to provide Human Resources information and system support for the DoD civilian workforce worldwide.

The system contains position authorization and control information; position descriptions and performance elements; personnel data and projected suspense information for personnel actions; pay, benefits, and entitlements data; historical information on employees, including job experience, education, training, and training transaction data; performance plans, interims, appraisals, closeouts and ratings; professional accounting or other certifications or licenses; awards information and merit promotion information; separation and retirement data; security information and adverse and disciplinary action data. Personnel information including, but not limited to: employee email address; employee phone numbers to include home, work, pager, fax and mobile; race and national origin; handicap code; and foreign language capability.

(2) Briefly describe the privacy risks associated with the PII collected and how these risks are addressed to safeguard privacy.

The primary privacy risk associated with this system is the risk of PII becoming compromised. This risk comes from the same threat sources that apply to all DoD information systems. These risks are addressed through the application of the DoD Defense Information Assurance Certification and Accreditation Process (DIACAP) and through DoD policies, procedures, and operational best practices. All individuals with privileged access to this system have appropriate background investigations and clearances for their position. Systems software and hardware are configured in accordance with DoD security guidance. All users must have current Privacy Act training.

h. With whom will the PII be shared through data exchange, both within your DoD Component and outside your Component (e.g., other DoD Components, Federal Agencies)? Indicate all that apply.

☒ **Within the DoD Component.**

Specify. The information is used by the Component HR community, employees and supervisors; the information is also passed in a 2-way interface from DCPDS to the staffing tool, RESUMIX for external recruitment and internal merit promotion.

☒ **Other DoD Components.**

Specify. As employees are transferred between DoD Components, their HR records are transferred. Also, PII is provided to DMDC, DEERS, J-PAS, DIMHRS, DMHRSi, DFAS, Army & Air Force NAF payroll to support their requirements. Currently the National Guard Bureau has two interfaces with Air Force and Army to get military information into DCPDS. These are National Guard Bureau employees who can be Military Reservists or Military Technicians that also work as Civilian employees. DIHMRS is replacing the two interfaces and will be providing the same data to DCPDS.

☒ **Other Federal Agencies.**

Specify. Information is used to generate reports required by the Office of Personnel Management.

☐ **State and Local Agencies.**

Specify.

☒ **Contractor** (Enter name and describe the language in the contract that safeguards PII.)

Specify. TALX, Avue Digital Services

☐ **Other** (e.g., commercial providers, colleges).

Specify.

i. Do individuals have the opportunity to object to the collection of their PII?

☒ **Yes** ☐ **No**

(1) If "Yes," describe method by which individuals can object to the collection of PII.

Privacy Act Statement (PAS) is provided on individual forms.

(2) If "No," state the reason why individuals cannot object.

j. Do individuals have the opportunity to consent to the specific uses of their PII?

☒ **Yes** ☐ **No**

(1) If "Yes," describe the method by which individuals can give or withhold their consent.

Additional PAS is provided before employees update their DCPDS employment related information through the Self Service Employee "MyBiz" module which is located within DCPDS.

(2) If "No," state the reason why individuals cannot give or withhold their consent.

k. What information is provided to an individual when asked to provide PII data? Indicate all that apply.

☒	**Privacy Act Statement**	☐	**Privacy Advisory**
☐	**Other**	☐	**None**

Describe each applicable format.

"The information you provide to the Defense Civilian Personnel Data System (DCPDS) is covered by the Privacy Act of 1974. For questions regarding your personal information please contact your local Human Resources Office.

Authorities: 5 USC 301; Title 5, USC Chapters 11, 13, 29, 31, 33, 41, 43, 51, 53, 55, 61, 63, 72, 75, 83, and 99; 5 USC 7201; 10 USC 136; 29 CFR 1614.601; and E.O.9397.

Principal Purposes: To allow civilian employees in the Department of Defense (DoD) to update personal information.

Routine Uses: None. The DoD 'Blanket Routine Uses' set forth at the beginning of OSD's compilation of systems of records notices apply to this system.

Disclosure: Voluntary. However, failure to provide or update your information may require manual HR processing or the absence of some information."